

Masashi TAKUBO, S.N. 10/766,724
Page 12

Dkt. 2271/71526

REMARKS

The application has been reviewed in light of the Office Action dated May 19, 2008. Claims 1-12, 14, 15, 17, 18 and 20 were pending, with claims 13, 16 and 19 having previously been canceled, without prejudice or disclaimer. By this Amendment, claims 1-10 and 20 have been amended to clarify the claimed subject matter, and new claim 21 has been added. Accordingly, claims 1-12, 14, 15, 17, 18, 20 and 21 are now pending, with claims 1-10 being in independent form.

Claims 1, 4, and 7 were rejected under 35 U.S.C. § 103(a) as purportedly unpatentable over U.S. Patent No. 7,023,573 to Ohhashi et al. in view of U.S. Patent No. 7,107,395 to Ofek et al. and further in view of U.S. Patent No. 5,958,005 to Thorne et al. Claims 2, 5 and 8 were rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek. Claims 3, 6, and 9 were rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek and further in view of Simpson et al. (US 20040036907 A1). Claims 10, 17, and 18 were rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek. Claims 11, 12, 14 and 15 were rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek and Thorne et al and further in view of well-known principles in the art of image processing. Claim 20 was rejected under 35 U.S.C. 103(a) as purportedly unpatentable over Ohhashi in view of Ofek and Thorne and further in view of U.S. Patent No. 6,757,698 to McBride.

Applicant has amended independent claims to clarify some of the aspects of the claimed subject matter that are neither taught nor suggested by the cited art. Applicant respectfully requests the Examiner to focus on such differences which are further elaborated below.

Determining whether received document image data is confidential

Masashi TAKUBO, S.N. 10/766,724
Page 13

Dkt. 2271/71526

Contrary to the contention in the Office Action, Ohhashi does not disclose or suggest determining whether received document image data is confidential.

Ohhashi, as understood by applicant, proposes an image transmission device configured to compare image data from a scanned document image with one or more specific pre-registered documents (that is, paper money, valuable securities, etc.), in order to detect a forgery of such pre-registered documents.

Ohhashi does NOT disclose or suggest anywhere that one of the specific pre-registered document contains confidential data and/or a scanned document image is compared with such pre-registered document to determine that the scanned document image contains confidential data.

Although the image transmission device of Ohhashi can transmit a document using a confidential communication mode, Ohhashi says NOTHING WHATSOEVER regarding determining whether received document image data is confidential.

As previously pointed out, the specific pre-registered documents (that is, paper money, valuable securities, etc.) that Ohhashi is concerned with detecting are not confidential at all but rather typically changes hands between transacting parties as forms of liquid assets.

The other references likewise do not disclose or suggest determining whether received document image data is confidential.

Thorne, as understood by Applicant, proposes an approach for allowing e-mail communications between computers connected to a network, while providing selectable degrees of security for each message. The motivation of Thorne is to allow communication of confidential data in a secure manner wherein a header of the e-mail communication specifies, in addition to the address of the intended destination, one or more security parameters (such as

Masashi TAKUBO, S.N. 10/766,724
Page 14

Dkt. 2271/71526

instructions for erasure of the data message following its storage in the recipient computer, instructions as to whether copying, archiving, forwarding and printing of the data message is permitted, etc.) which control the processing of the e-mail at the destination.

However, the receiving side of the communication system proposed by Thorne does **NOT** determine whether received document image data is confidential and then deny access to the received document image data if the received document image data is determined to be confidential. To the contrary, the receiving side merely follows the instructions included in the header of the received e-mail communication.

The aspect in the present application of determining whether received document image data is confidential is simply not disclosed, suggested or otherwise rendered obvious by the cited references.

**Storing copies of image data in
first and second image data storing mechanism, respectively**

The cited art also fails to disclose or suggest storing received document image data into a first image data storing mechanism inaccessible through the local area network, and only if the received document data is determined to be not confidential, allowing a copy of the received document image data to be stored in a second image data storing mechanism accessible through the local area network.

Memory 23 in Fig. 7 of Ohhashi is equated in the Office Action with a first storing mechanism.

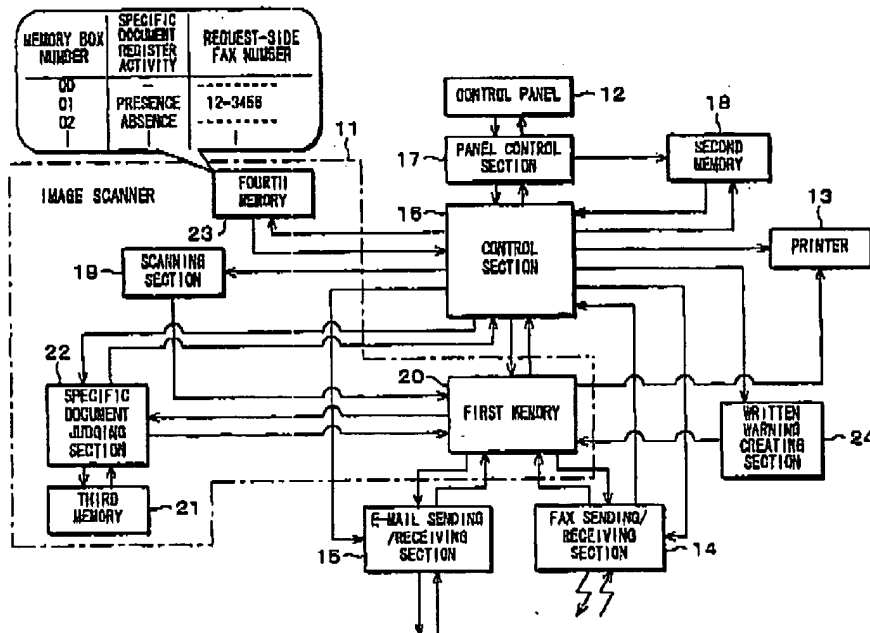
The memory 23 in Fig. 7 of Ohhashi, as shown in Fig. 2 (reproduced below) thereof and as discussed at column 12, lines 27-42, is configured as a plurality of memory boxes, and each memory box is assigned to a corresponding registered (that is, scanned) document and is used for storing specific document register information indicating whether the specific document is a

Masashi TAKUBO, S.N. 10/766,724
Page 15

Dkt. 2271/71526

forgeries and storing a facsimile number of the transmission destination.

FIG. 2



Although an unused memory might be configured to store image data, the memory 23 of Ohhashi is allocated for storing specific data that is **NOT** image data, and such memory 23 is simply **NOT** configured for storing image data representing a document image.

Further, it is noted that Ohhashi is not concerned with determining whether the received document image data (representing the received document) is confidential, and restricting access to the received document image data if it is determined to be confidential.

The objective of Ohhashi is to detect whether scanned documents are forgeries of valuable documents, such as paper money and valuable securities. The memory 23 in the transmission device of Ohhashi is allocated to store for each scanned document, information indicating whether such forgery is present in the document.

Stated another way, the memory 23 is coincidentally inaccessible through the local area

Masashi TAKUBO, S.N. 10/766,724
Page 16

Dkt. 2271/71526

network because it is allocated for storing internal data that is relevant only to the operation of the transmission device of Ohhashi and that is no concern to external devices. Ohhashi does not disclose or suggest that the memory 23 should be inaccessible through the local area network to keep external devices from having access to the data stored in the memory 23.

Thus, it would *NOT* have been obvious to one skilled in the art to modify the device of Ohhashi to store image data in the memory 23 such that image data that is confidential can be made inaccessible through the local area network.

Ofek, as understood by applicant, proposes a configuration of networked storage devices configured into a storage domain which can be accessed from host computers through a computer network to which the storage devices and host computers are connected. The storage devices include a plurality of primary storage devices and a secondary storage device, and the secondary storage device is coupled to the primary storage devices through the network to provide backup media for the host computers.

Thus, although Ofek proposes a backup mechanism, each of the storage mechanisms in the networked system of Ofek must be accessible through the network.

Ofek is not concerned with whether specific stored image data is confidential and allowing such confidential image data to be stored only in a storage mechanism that is inaccessible through the network.

Thus, Ofek, contrary to the contention in the Office Action, does not cure the deficiencies of Ohhashi.

The other cited references, like Ohhashi, Ofek and Thorne, do not disclose or suggest (a) determining whether received document image data is confidential, and (b) storing received document image data into a first image data storing mechanism inaccessible through the local

Masashi TAKUBO, S.N. 10/766,724
Page 17

Dkt. 2271/71526

area network, and only if the received document data is determined to be not confidential, allowing a copy of the received document image data to be stored in a second image data storing mechanism accessible through the local area network.

Simpson, as understood by Applicant, proposes a system wherein a facsimile message is saved through a network (the Internet) to a personal image repository as a facsimile image in a format compatible with multiple computer operating systems for use with an identity-based imaging system.

McBride, as understood by Applicant, proposes an approach for automatically synchronizing data from a host computer to two or more backup data storage locations.

McBride, like the other cited references, does not disclose or suggest a first storing mechanism configured to store image data representing a document image and to be inaccessible through the local area network.

Simpson and McBride, like the other references, are not concerned with whether specific stored image data is confidential and allowing such confidential image data to be stored only in a storage mechanism that is inaccessible through the network.

Accordingly, applicant submits that the cited art, even when considered along with common sense and common knowledge to one skilled in the art, does **NOT** render unpatentable the subject matter of independent claims 1-10 of the present application.

In view of the remarks hereinabove, Applicant submits that the application is in condition for allowance. Accordingly, Applicant earnestly solicits the allowance of the application.

If a petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition. The Patent Office is hereby authorized to charge any fees that are required in connection with this amendment and to credit any overpayment to our

Masashi TAKUBO, S.N. 10/766,724
Page 18

Dkt. 2271/71526

Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Respectfully submitted,



Paul Teng, Reg. No. 40,837
Attorney for Applicant
Cooper & Dunham LLP
Tel.: (212) 278-0400